The Ultimate Guide for Anonymous and Secure Internet Usage v1.0.1

By

cyberguerrilla.info

Table of Contents:

Foreword

By the time you are finished reading and implementing this guide, you will be able to securely and anonymously browse any website and to do so anonymously. No one not even your ISP or a government agent will be able to see what you are doing online. If privacy and anonymity is important to you, then you owe it to yourself to follow the instructions that are presented here.

In order to prepare this guide for you, I have used a computer that is running Windows Vista. This guide will work equally well for other versions of Windows. If you use a different operating system, you may need to have someone fluent in that operating system to guide you through this process. However, most parts of the process are easily duplicated in other operating systems.

I have written this guide to be as newbie friendly as possible. Every step is fully detailed and explained. I have tried to keep instructions explicit as possible. This way, so long as you patiently follow each step, you will be just fine.

In this guide from time to time you will be instructed to go to certain URLs to download files. You do NOT need TOR to get these files, and using TOR (while possible) will make these downloads very slow.

This guide may appear overwhelming. Every single step is explained thoroughly and it is just a matter of following along until you are done. Once you are finished, you will have a very secure setup and it will be well worth the effort. Even though the guide appears huge, this whole process should take at the most a few hours. You can finish it in phases over the course of several days.

It is highly recommended that you close *ALL* applications running on your computer before starting.

=== 1: Obtaining Tor Browser ===

The first step to becoming secure and anonymous online is to setup and install something called “TOR”. “TOR” is short for “The Onion Router”. The concepts behind TOR were first implemented by the United States Military, and these principles have been used to create an extremely secure mechanism for being anonymous online. In fact, millions of people world-wide use TOR to browse the internet and communicate anonymously.

TOR works by heavily encrypting your communications so that no observer can see what website you are really going to, and what information is really being sent. It all appears as a bunch of random characters to any observer. You simply use the TOR web browser just as you use any other web browser. TOR takes care of the rest.

However, TOR by itself is not enough. Even when using TOR, a user can be compromised in a number of ways. First, some websites can be set up to attempt to reveal someone’s true IP address (their true identity) by tricking their web browser or other software to transmitting that information. For this reason, anyone who uses TOR will recommend that no one have JavaScript or flash turned on while browsing TOR. In this guide however, I will show you a much better solution.

The second issue is that of human error. Even if you have TOR installed, you may accidentally forget which browser to put in a link. You may also accidentally click on a link from another program, such as a chat program. That program might then load the link you clicked on into a non-TOR browser. When you are using TOR, you must be careful *constantly* that every link goes into the right browser, and that you do not accidentally click the wrong link.

So then, let’s begin. Obtaining the TOR Browser is easy. Simply go to the following website:

http://www.torproject.org

Once here, you may feel free to read more about what TOR is and how it works, or you may proceed to immediately download TOR.

Here is how to do so:

1. Click on “Download TOR”, or “Download”.
2. You will see text that says, “The Tor Browser Bundle contains everything you need … Just extract it and run. Learn more >>
3. Click on this “Learn more” link. for the “Tor Browser Bundle”

4. Assuming you are an English speaker, you would choose the top-most link “English (en-US)”. Otherwise, pick the language best suited to you.
5. The file being saved will be named: tor-browser-1.3.18_en-US.exe It is ok if the number is not exactly 1.3.18, there are new versions of Tor from time to time. At the time that this guide was written, 1.3.18 was most current. By the time you are reading this, a more current version of TOR may exist.
6. Run this file.
7. You will be prompted to extract this to a directory. By default, it will be set to C:UsersYourDownloads This is perfectly ok. You can also choose a different directory if you wish.
8. Click “Extract”

That’s it. TOR Browser is NOW installed. Time to test it out!

=== 2: Using and Testing Tor Browser for the first time ===

Now you have successfully downloaded and installed the Tor Web Browser Bundle. You are no doubt anxious to begin using it. First, click on the “start” menu icon, the icon in the lower left of your screen with the windows logo. On the top right will be a listing that says “You”, “Documents”, “Pictures”, “Music”… “You” of course will be replaced by your user name. Click on “You”, the top most link. This will open up your main user folder.

Now, locate the folder called “Downloads” and double click on it.

Now, inside the “Downloads” folder, double click on the folder called “Tor Browser”.

Lastly, double click on the application: “Start Tor Browser”

When you do, you will see the Vidalia Control Panel appear, and you will observe as you connect to the TOR network. When this is complete, your web browser will open up and will automatically connect to the web address: check.torproject.org

This is to confirm that you are in fact using TOR. If you have followed this guide correctly, then you will see the following green text, or something similar:

“Congratulations. Your browser is configured to use Tor.”

Now you can use this web browser the same as any other. You can go to any website you wish, and neither your ISP nor anyone else will be able to see where you are going, or what you are doing. However, there are still issues that need to be resolved, so don’t begin browsing just yet.

****

***** IMPORTANT SAFETY NOTE *****

****

If you fill out a form containing your email address, your name, or any other sensitive information while using the TOR browser, be aware that sometimes it is possible for an observer to see that information. When using TOR, use it to access websites and content that you are *not* connected to via your real identity or any username or nick name which links to your real identity. Let TOR be for anonymous browsing solely. Do your online banking, or any other activities involving your real identity using your normal web browser.

=== 3: Securing Your Hard Drive ===

Being able to browse anonymously is one thing. However, you may choose to download and save sensitive content or material to your computer which you wish to keep private. This may include reading sensitive documents, viewing pictures, or storing any kind of sensitive data.

If you save *anything* to your computer's hard drive, then it is possible for someone who has confiscated your computer to determine what it was you saved. This is often true even if you delete the content. For example, suppose I use the Tor Browser and I navigate to a website containing a sensitive document that I wish to read. If I saved that document somewhere on my harddrive, then it is possible for someone else to find it. If I *delete* that document, it may still be possible for someone to undelete it.

Further, even if I never save it to my hard drive but I simply look at it using my word processing software, it may still be saved in a number of ways including:

1. Often programs keep records of filenames. The filename alone is often enough to incriminate someone.

2. Often programs keep parts of the content viewed saved for various reasons, such as for searching. This can include random excerpts of text, thumbnails of images, and more. Often this "partial" data is more than enough to prove what the original data was. Often the "partial" data is itself incriminating.

3. Sometimes, especially if you are running low on system memory, your operating system may choose to use your hard-disk as a temporary RAM. This is known as "SWAP". Normally, whenever you turn off your computer, whatever was in RAM is deleted. However, the data that goes to your SWAP may persist and it may be possible for someone to see what content you had open in your programs if that information is saved in RAM.

Generally speaking, you *must* have a plan to secure any content that is saved to your hard disk. Therefore, this guide would be incomplete if we did not thoroughly address this. First, there are two kinds of such content:

1. Deliberately saved content.

2. Inadvertently saved content.

Deliberately saved content refers to content that you have chosen to save on your hard disk so that you can access this content later. We will address how to do this later in the guide.

Inadvertently saved content refers to content that is saved by programs you use, or your operating system. You have no way to even know what this content might be. Therefore, this is the most dangerous. You may browse and find a dozen sensitive documents, utterly delete them, and some program may have saved the file names and excerpts of the data. This will render your previous efforts futile.

Content that is inadvertently saved to your hard disk comes in two flavors:

1. Content that is saved to your SWAP space.

2. Content that is saved by applications running on your computer, including your operating system.

The surest way to prevent content from writing to your SWAP space is to disable your SWAP space altogether. This may result in your computer

running a bit slower than normal, and may mean that you cannot use ram intensive games and applications during the time your SWAP is disabled.

Therefore, if you use this method, simply turn back on the SWAP when you want to use those ram intensive applications. Also, you may choose not to take this step.

1 – Here is how to disable your swap space if you are using Windows 7:

*** ADVANCED INSTRUCTIONS BELOW. SKIP THIS IF YOU ARE NOVICE OR UNCOMFORTABLE WITH THIS OPERATION ***

This step is recommended for advanced users only. If you are not comfortable doing this, you may safely skip this step.

Instructions are less verbose than usual, as these steps are intended for advanced users only. If you do not fully understand these instructions, skip this step.

From Control Panel, go to “System and Security”.

Click on “System”, and then choose “Advanced system settings” in the left-most menu.

Under the “Advanced” tab, under “Performance”, click “Settings”.

Under this “Advanced” tab, under “Virtual Memory”, click “Change”.

Uncheck “Automatically manage paging file sizes for all drives”.

Select “No paging file”.

Save, reboot, and follow these same first 5 steps to confirm that “No paging file” is still selected. This means that you have successfully disabled your swap. This means that *nothing* from RAM will be inadvertently saved to your hard drive.

To resume using SWAP again, simply click “Automatically manage paging file size for all drives.” You can switch between these two modes as you desire.

Generally speaking, your computer will run fine without a swap file, provided you have enough RAM.

*** END OF ADVANCED INSTRUCTIONS ***

The next issue we need to address is how to prevent applications and/or your operating system from saving content inadvertently that you do not want saved. For this, we are going to set up a “Virtual Machine”.

A “Virtual Machine” is like a computer inside of your computer. Everything you do inside the Virtual Machine (vm for short) will be fully contained within itself and no one will be able to see what the vm has been doing. Ideally, you want *ALL* of your sensitive computer usage of any kind, TOR or NON TOR, to take place within a VM. In this way, you can keep everything private that you wish while still using your computer fully and getting the most out of it.

Don’t be afraid of this sounds complicated. This guide will take you through every step slowly and methodically. Before we can set up a vm however, we need to take another step.

=== 4: Setting up TrueCrypt, Encrypted Hidden Volumes ===

If you save anything on your computer, it is likely that you do not want just anyone to be able to see what you have saved. You want a way to protect that information so that you can access it, and absolutely no one else except those you trust. Therefore, it makes sense to set up a system which protects your information and safeguards it against prying eyes.

The best such system for this is called “True Crypt”. “True Crypt” is an encryption software program which allows you to store many files and directories inside of a single file on your hard drive. Further, this file is encrypted and no one can actually see what you have saved there unless they know your password.

This sounds extremely high tech, but it is actually very easy to set up. We are going to do so, right now:

1. Go to http://www.truecrypt.org/downloads (or go to http://www.truecrypt.org and click on “Downloads”)

2. Under “Latest Stable Version”, under “Windows 7/Vista/XP/2000″, click “Download”

3. The file will be called “True Crypt Setup 7.0a.exe” or something similar. Run this file.

4. If prompted that a program needs your permission to continue, click “Continue”.

5. Check “I accept and agree to be bound by these license terms”

6. Click “Accept”

7. Ensure that “Install” is selected, and click “Next”

8. click “Install”

9. You will see a dialog stating “TrueCrypt has been successfully installed.” Click “Ok”

10. Click “No” when asked if you wish to view the tutorial/user’s guide.

11. Click “Finish”

At this point, TrueCrypt is now installed. Now we will set up truecrypt so that we can begin using it to store sensitive information.

1. Click the “Windows Logo”/”Start” button on the lower left corner of your screen.

2. Click “All Programs”

3. Click “TrueCrypt”

4. Click the “TrueCrypt” application

And now we can begin:

1. Click the button “Create Volume”

2. Ensuring that “Create an encrypted file container” is selected, click “Next”

3. Select “Hidden TrueCrypt volume” and click “Next”.

4. Ensuring that “Normal mode” is selected, click “Next”

5. Click on “Select File”

    Note which directory you are in on your computer. Look at the top of the dialog that has opened and you will see the path you are in, most likely the home directory for your username. An input box is provided with a flashing cursor asking you to type in a file name. Here, you will type in the following filename:

    random.txt

    You may of course replace random.txt with anything you like. This file is going to be created and will be used to store many other files inside.

    Do NOT use a filename for a file that already exists. The idea here is that you are creating an entirely new file.

    It is also recommended though not required that you “hide” this file somewhere less obvious. If it is in your home directory, then someone who has access to your computer may find it easier. You can also choose to put this file on any other media, it doesn’t have to be your hard disk. You could for example save your truecrypt file to a usb flash drive, an sd card, or some other media. It is up to you.

6. Once you have typed in the file name, click “Save”

7. Make sure “Never save history” is checked.

8. Click “Next”

9. On the “Outer Volume” screen, click “Next” again.

10. The default Encryption Algorithm and Hash Algorithm are fine. Click “Next”

11. Choose a file size.

    In order to benefit the most from this guide, you should have at least 10 gigabytes of free disk space. If not, then it is worth it for you to purchase some form of media (such as a removable hard drive, a large SD card, etc.) in order to proceed. TrueCrypt can be used on all forms of digital media not just your hard disk. If you choose to proceed without obtaining at least ten gigabytes of disk space, then select a size that you are comfortable with….

    (Such as 100 MB).

    Ideally, you want to choose enough space to work with. I recommend 20 GB at least. Remember that if you do need more space later, you can always create additional TrueCrypt volumes using exactly these same steps.

12. Now you are prompted for a password. THIS IS VERY IMPORTANT. READ THIS CAREFULLY

*** READ THIS SECTION CAREFULLY ***

*** The password you choose here is a decoy password. That means, this is the password you would give to someone under duress. Suppose that someone suspects *** that you were accessing sensitive information and they threaten to beat you or worse if you do not reveal the password. THIS is the password that you *** give to them. When you give someone this password, it will be nearly impossible for them to prove that it is not the RIGHT password. Further, they cannot *** even know that there is a second password.

Here are some tips for your password:

A. Choose a password you will NEVER forget. It may be ten years from now that you need it. Make it simple, like your birthday repeated three times.

B. Make sure it seems reasonable, that it appears to be a real password. If the password is something stupid like “123″ then they may not believe you.

C. Remember that this is a password that you would give to someone if forced. It is *NOT* your actual password.

D. Do not make this password too similar to what you plan to really use. You do not want someone to guess your main password from this one.

And with all of this in mind, choose your password. When you have typed it in twice, click “Next”.

13. “Large Files”, here you are asked whether or not you plan to store files larger than 4 GIGABYTES. Choose “No” and click “Next”

14. “Outer Volume Format”, here you will notice some random numbers and letters next to where it says “Random Pool”. Go ahead and move your mouse around for a bit. This will increase the randomness and give you better encryption. After about ten seconds of this, click “Format”.

15. Depending on the file size you selected, it will take some time to finish formatting.

“What is happening?”

TrueCrypt is creating the file you asked it to, such as “random.txt”. It is building a file system contained entirely within that one file. This file system can be used to store files, directories, and more. Further, it is encrypting this file system in such a way that without the right password it will be impossible for anyone to access it. To *anyone* other than you, this file will appear to be just a mess of random characters. No one will even know that.

It is a TrueCrypt volume.

16. “Outer Volume Contents”, click on the button called, “Open Outer Volume”

An empty folder has opened up. This is empty because you have yet to put any files into your truecrypt volume.

*** *** DO NOT PUT ANY SENSITIVE CONTENT HERE *** ***

This is the “Decoy”. This is what someone would see if you gave them the password you used in the previous step. This is NOT where you are going to store your sensitive data. If you have been forced into a situation where you had to reveal your password to some individual, then that individual will see whatever is in this folder. You need to have data in this folder that appears to be sensitive enough to be protected by truecrypt in order to fool them. Here are some important tips to keep in mind:

A. Do NOT use porn. Adult models can sometimes appear to be under aged, and this can cause you to incriminate yourself unintentionally.

B. Do NOT use drawings/renderings/writings of porn. In many jurisdictions, these are just as illegal as photographs.

C. Good choices for what to put here include: backups of documents, emails, financial documents, etc.

D. Once you have placed files into this folder, *NEVER* place any more files in the future. Doing so may damage your hidden content.

Generally, you want to store innocent data where some individual looking at it would find no cause against you, and yet at the same time they would understand why you used TrueCrypt to secure that data.

Now, go ahead and find files and store them in this folder. Be sure that you leave at least ten gigabytes free. The more… The better.

When you are all done copying files into this folder, close the folder by clicking the “x” in the top right corner.

17. Click “Next”

18. If prompted that “A program needs your permission to continue”, click “Continue”

19. “Hidden Volume”, click “Next”

20. The default encryption and hash algorithms are fine, click “Next”

21. “Hidden Volume Size”, the maximum available space is indicated in bold below the text box. Round down to the nearest full unit. For example, if 19.97 GB is available, select 19 GB. If 12.0 GB are available, select 11 GB.

22. If a warning dialog comes up, asking “Are you sure you wish to continue”, select “Yes”

23. “Hidden Volume Password”

*** IMPORTANT READ THIS ***

Here you are going to select the REAL password. This is the password you will NEVER reveal to ANYONE else under any circumstances. Only you will know it. No one will be able to figure it out or even know that there is a second password. Be aware that an individual intent on obtaining your sensitive information may lie to you and claim to be able to figure this out. They cannot.

It is HIGHLY recommended that you choose a 64 character password here. If it is difficult to remember a 64 character password, choose an 8 character password and simply repeat it 8 times. A date naturally has exactly 8 numbers, and a significant date in your life repeated 8 times would do just fine.

24. Type in your password twice, and click “Next”

25. “Large Files”, select “Yes” and click “Next”.

26. “Hidden Volume Format”, as before move your mouse around for about ten seconds randomly, and tehn click “Format”.

27. If prompted “A program needs your permission to continue”, select “Continue”

28. A dialog will come up telling you that the hidden TrueCrypt volume has been successfully created. Click “Ok”

29. Click “Exit”

Congratulations! You have just set up an encrypted file container on your hard drive. Anything you store here will be inaccessible to anyone except you. Further, you have protected this content with TWO passwords. One that you will give to someone under threat, and one that only you will know. Keep your real password well protected and never write it down or give it to anyone else for any reason.

Now, we should test BOTH passwords.

=== 5. Testing TrueCrypt Volumes ===

Once you have completed the above section, you will be back at TrueCrypt. Go ahead and follow these steps to test the volumes you have made.

1. Click “Select File…”

2. Locate the file you created in the last section, most likely called “random.txt” or something similar. Remember that even though there is both an outer and

a hidden volume, both volumes are contained in a single file. There are not two files, only one.

3. Click “Open”

4. Choose a drive letter that you are not using (anything past M is probably just fine). Click on that, For example click on “O:” to highlight it.

5. Click “Mount”

6. Now you are prompted for a password. Read the below carefully:

> The password you provide here will determine WHICH volume is mounted to the drive letter you specified. If you type in your decoy password, then O: will show all the files and directories you copied that you would reveal if forced. If you type in your real password, then O: will show the files and directories that you never intend anyone to see.

7. After successfully typing in your password, you will see additional detail to the right of the drive letter, including the full path to the file you selected as well as the kind of volume it is (for example, hidden).

8. Right click on your “Windows Logo”/”Start Menu” icon, and scroll down to the bottom where you can see your different drive letters. You will see the drive letter you selected, for example: “Local Disk (O:)”. Click on that.

9. If you selected your decoy password, you will see all the files and folders that you moved there during the installation phase. If you selected the real password, you will see whatever files and directories you have placed so far into the hidden volume, if any.

If you selected your hidden volume password, you may now begin moving any sensitive information you wish. Be aware that simply moving it from your main hard disk is not

enough. We will discuss how to ensure deleted data is actually deleted later in the guide.

“What is happening?”

When you select a file and mount it to a drive, you are telling your computer that you have a new drive with files and folders on it. It is the same thing as if you had plugged in a usb flash drive, a removable harddrive, or an sd card into your computer. TrueCrypt causes your computer to think that there is an entirely new disk drive on your computer. You can use this disk drive just as if it *was* actually a usb flash drive. You can copy files to it, directories, and use it just as you would use a usb flash drive.

When you are done, simply close all open windows/folders/applications that are using your truecrypt drive letter, and then click “Dismount” from within TrueCrypt while you have the drive letter highlighted. This will once again hide all of this data, accessible only by re-mounting it with the correct password.

*** VERY IMPORTANT SAFETY INFORMATION ***

When a true crypt hidden volume is mounted, someone who has access to your computer can access anything that is inside that hidden volume. If for example you left your computer running while a truecrypt volume was mounted, then if someone gained access to your computer they would be able to see everything you have in that volume. Therefore:

*** ALWAYS REMEMBER TO DISMOUNT ANY TRUECRYPT VOLUME CONTAINING ANY SENSITIVE INFORMATION WHEN YOU ARE NOT USING YOUR COMPUTER ***

You can tell that it is dismounted because the drive letter inside of “TrueCrypt”‘s control panel will appear the same as all of the other drive letters, with no information to the right of the drive letter.

You should practice Mounting and Dismounting a few times with both passwords to make sure you understand this process.

Once you have copied files/folders into the hidden volume, do *NOT* touch the files or folders in the outer volume anymore. Remember that both volumes occupy the same single file, and therefore changing the outer volume can damage the hidden volume. Once you have copied files/folders into the outer volume during the installation process, that is the last time you should do so. From that point forward, use ONLY the hidden volume. The outer volume exists only as a decoy if you need it.

=== 6. Securing your Disk ===

This is an involved step which many people may not be able to do right away. If you cannot do this step immediately, then see section 7.

At this point you should understand how to create and use TrueCrypt hidden volumes in order to safeguard any sensitive information. Therefore, you should *NOT* keep any such sensitive information on your hard disk.

At this stage, there are two possibilities:

1. You have never had any sensitive information on your hard disk. In this case, read this section but you can certainly skip it.

2. Up until now, you have stored sensitive information on your hard disk. If so, then you MUST read this section.

If you have ever used this computer to access sensitive information, then all of the security and precautions in the world are totally useless and futile because all someone has to do is access what is left of that sensitive information. I cannot stress this enough.

You can have the most secure TrueCrypt volumes, use TOR, and be the safest most secure user in the world. If you have not made sure that *ALL* remnants of any sensitive information are UTTERLY REMOVED from your hard disk, then all of that effort is totally pointless. You MUST take these actions to safeguard your hard disk, or otherwise you might as well throw away this guide and follow none of the advice herein.

First, I understand that it is troublesome to have to re-format a computer, to back everything up, and reinstall everything. However, if you have ever had sensitive information on your machine, which is what you, have to do. Take the following steps:

1. Obtain a removable hard drive or USB flash drive large enough to store anything you need to save.

2. Set up a TrueCrypt hidden volume on that hard drive big enough to hold all of that information.

3. Set up the TrueCrypt outer volume as in the previous section. Use the previous section as a guide if you need to.

4. Be sure you the hidden volume will have enough space to store all that you are backing up.

5. Copy ALL data you need to back up/save into that hidden volume.

*** IMPORTANT, READ THIS ***

If you have ever used this system to access sensitive information, then you must assume that the sensitive information or remnants of it can be *anywhere* on your hard disk. Therefore, you need to move *EVERYTHING* you intend to save into the hidden TrueCrypt container. You do not know where sensitive data might be, so you are assuming it can be anywhere. This way you still have ALL of your data and you have lost nothing.

A good analogy is toxic waste. You don't know which barrel might contain the toxic waste, so you treat *ALL* the barrels as potentially toxic. This is the surest way you can protect yourself.

You might be saying, "I have family photos, music, movies that I would have to move to the hidden volume." That is perfectly fine. Remember that you can access that hidden volume just as if it was a drive letter. In fact, ideally, *ALL* of the content on your computer (assuming you value your privacy) should be protected anyways. You lose nothing by securing all of that data.

6. Once you have copied everything you intend to copy. dismount your hidden volume, reboot your computer, and re-mount your hidden volume to make sure everything is there.

7. Now it is time to re-format your entire hard drive. Re-install your operating system of choice (such as Windows 7), and start with a clean slate.

8. Once you have reinstalled your operating system from scratch, follow sections one through five of this guide to reach this point, and then proceed.

=== 7. Temporarily Securing Your Disk, Shredding Free Space ===

Like the previous section, this section applies ONLY IF there is some risk that sensitive data has ever been stored or accessed on this computer. If you are 100% sure that sensitive information has never been accessed using this computer, then you can safely skip this and the previous step.

If you are not prepared to take the actions in the previous step yet, then you should follow the steps in this section until you can. However, you MUST eventually take the actions in step six above. Do not assume you can find/delete all sensitive content. Lists of filenames, image thumbnails, random data, and more *ARE* sitting on your hard disk. Someone who knows how to find it, WILL. That will render all of your other precautions totally futile.

As soon as you can, follow the instructions in step six.

Meanwhile, here is how you can temporarily safeguard yourself until you are able to follow those instructions.

1. Go through your hard disk folder by folder, deleting (or moving to a truecrypt hidden volume) any files that you believe are sensitive/risky.

2. When you are totally sure that you have deleted all such files, go to the following URL: http://www.fileshredder.org

3. Scroll down and look for the button called “Download File Shredder” — do NOT click any other button, as the page may have ads on it that appear to be download links.

4. Save the file.

5. Run the file, most likely titled: file_shredder_setup.exe

6. “Welcome to the File Shredder Setup Wizard”, Click “Next”

7. Select “I accept the agreement” and click “Next”

8. It will choose where to install it, click “Next”

9. Click “Next” again when prompted for the Start Menu folder.

10. “Select Additional Tasks”, Click “Next” again

11. Click “Install”

12. Ensuring that “Launch File Shredder” is checked, click “Finish”

13. You should now notice that “File Shredder” is running. You should see the program in your task bar. Click on it to bring up the control panel if it is not up already.

14. On the left is a link that says “Shred Free Disk Space”, click it.

15. Choose the drive letter for your hard disk, typically C:, as well as any other drives you wish to shred the free space.

16. under “Select Secure Algorithm”, select “Secure Erasing Algorithm with 7 passes” and click “Next”

17. Click “Start”

This will take some time to finish. Once you have finished shredding your free disk space, it will be impossible or nearly impossible for someone to find one of your deleted files and piece it back together to see what it once was. However, this is NOT enough.

Keep in mind that there may still be records of the filenames that were deleted, partial data from those files, image thumbnails, and more that may be enough to incriminate you. This is only a temporary step you have taken, and you absolutely must take the actions in step 6 above in order to be truly safe.

=== 8. Installing VirtualBox ===

And now we get to the fun part. We are going to create a secure environment for you to browse the internet and communicate in a way that is totally anonymous and untraceable. You will have a setup that is so secure as to be virtually impossible to break.

1. First, go to the following URL: http://www.virtualbox.org

2. Select “Downloads” in the menu on the left.

3. Under “VirtualBox platform packages” is “VirtualBox 4.0.4 for Windows Hosts”, next to that is “x86/amd64″. Click that.

4. Save the file. It should be titled similar to: “VirtualBox-4.0.4-7011-Win.exe

5. Run the file.

6. “Welcome to the Oracle VM… Setup Wizard”, Click “Next”

7. Click “Next”

8. Click “Next”

9. “Warning: Network Interfaces”, click “Yes” but be aware that your internet connection will be temporarily reset for a few seconds.

10. Click “Install”

11. A dialog saying “A program needs your permission to continue” may appear, click “Continue”.

12. One or more dialogs asking if you want to install “device software” may come up, select “Install” each time.

13. Optionally check the box “Always trust software from Oracle Corporation.”

14. “Oracle VM… installation is complete”, Click “Finish” ensuring that “Start Oracle VM after installation” is checked.

Now we have the software we need in order to set up and run virtual machines. On your task bar to the far right, you should notice VirtualBox running. Click on the “VirtualBox” icon if needed in order to bring the VirtualBox control panel into view.

Now it is time to set up a virtual machine. For this, we need to obtain two files. Operating systems, such as windows, are typically installed using a cd or dvd. You put the CD or DVD into your computer, you boot it up, and you follow the instructions in order to install the operating system. Virtual machines work similarly. Before we can use a virtual machine, we have to install an operating system on it.

However, we are *NOT* going to use Windows! We are going to use Linux. Do not be afraid if you have no experience using Linux. I assure you that this will prove to be painless. We actually need two different linux operating systems in order to have a secure system. Before we go through the steps of setting this up, I want to describe to you what we are doing.

Remember earlier in the guide I explained that one of the downsides to using Tor Browser from your main computer is that you might accidentally put a link into a non-Tor browser. The problem with your computer right now is that you can access tor sites, or non-tor sites equally well. That means that you have to be extremely careful to ensure that you are using Tor.

An analogy would be to say that you are typing on a keyboard with red and green keys. You have to be careful to only hit the green keys. If you accidentally hit a red key, then you could compromise your security and anonymity. That is *not* a good position to be in. The purpose of setting up a virtual machine is to make certain that you cannot accidentally reveal your identity or compromise your security.

The computer you are using now has two ways of accessing the internet: TOR, and Non-TOR. The Virtual Machine we are setting up however will only be able to access the internet using TOR. No other way period. That means that no matter what you do, no matter how hard you try, you will NOT be able to accidentally access any website except through TOR. This *guarantees* that whatever you do on that virtual machine is going to be through TOR.

So how do we achieve this? There are a number of ways to do so. The method presented in this guide is not the only good way, however I do believe that it is both easy to set up and also friendly to users who may not have a great deal of RAM.

First, we are going to set up two different virtual machines. One of them will exist for the sole purpose of making sure that the other one does not accidentally connect to the internet except through TOR. This virtual machine requires very little. You will not be using it for anything. It will simply act as a gatekeeper to ensure that the other Virtual Machine is safe.

The second virtual machine will be what you use for internet browsing, chatting, etc. This virtual machine will be configured in such a way that it can only use TOR and

nothing else. The way we will achieve this is to force this second virtual machine to go through the first virtual machine for all internet connections.

Do not worry if this seems complicated. As with the rest of this guide, I am going to walk you through step by step exactly what to do.

First, we have to obtain the operating systems we will need. In this case, we are going to use “Damn Small Linux” (yes that is it’s real name) for the firewall and we are going to use “Ubuntu” for the main system. The advantage to using “Damn Small Linux” is that we only need 32 MB of ram and no disk sapce to have an effective firewall.

Let’s set up the firewall first:

=== 9. Installing a Firewall ===

1. First, go to the following URL: http://www.damnsmalllinux.org (three l's)

2. Scroll down until you see a link that says "Download"

3. Under "Current Full Mirror List", click any that work. Some may not work at any given time. If one doesn't work, simply hit back on your browser and try another one.

4. At the time of this guide, the following url worked: ftp://ftp.is.co.za/linux/distributions/damnsmall/current/

5. Go to the "current" directory if not already in it.

6. Click on the file called: dsl-4.4.10.iso — If you cannot find this file, choose the file closet to it. A higher version number is fine. The file will probably be about 50 MB

7. The file should take about 5-10 minutes to download based on your connection.

(IF THE ABOVE STEPS WORKED FOR YOU, SKIP THIS MINI-SECTION)

(If you had trouble with the above steps, read this mini-section)

(With mirrors, it is often the case that a particular mirror site doesn't work. At the time of this writing, several mirrors worked. I am providing detailed instructions for each mirror.)

(Above I have already provided instructions for the mirror)

ftp://ftp.is.co.za

MIRROR: http://gd.tuwien.ac.at/opsys/linux/damnsmall

(Go to this URL, and under "Subdirectories" click on "current") if available, select the file called "current.iso" (provided the file is at least 49 MB in size) If not, then choose the closest file to dsl-4.4.10.iso, a higher version # is fine.

MIRROR: http://ftp.belnet.be/packages/damnsmalllinux/

(go to "current" directory, obtain either "current.iso" (if 49 MB or higher) or find file closest to "dsl-4.4.10.iso")

MIRROR: http://ftp.heanet.ie/mirrors/damnsmalllinux.org/

(go to “current” directory, obtain either “current.iso” (if 49 MB or higher) or find file closest to “dsl-4.4.10.iso”)

At this point, you should have the file either “current.iso” or “dsl-4.4.10.iso” (or something similar) fully downloaded and saved into your Downloads directory.

Now, go ahead and open up VirtualBox again, most likely by clicking it on the task bar.

8. Click “New” at the top left, an icon that resembles a many-pointed round star.

9. “Welcome to the New Virtual Machine Wizard”, click “Next”

10. “VM Name and OS Type”: Under “Name” type in: Firewall

11. For Operating System, choose “Linux”

12. For “Version”, choose: “Other Linux”

13. Click “Next”

14. “Memory”, select “32 MB” and click Next

15. “Virtual Hard Disk”, Uncheck “Boot Hard Disk” and click “Next”

16. If a Warning dialog appears, click “Continue”

17. Click “Finish”

18. Now you will notice “Firewall, Powered Off” visible in your VirtualBox control panel. Make sure it is highlighted (it should be) and then right click it, and select “Settings”.

19. Select “Network” in the menu to the left.

20. Click on the “Adapter 2″ tab.

21. Check “Enable Network Adapter” and next to where it says “Attached to”, select “Internal Network” from the pulldown menu.

22. Click “Ok” at the bottom.

23. Once again, right click “Firewall, Powered Off” and select “Start”

24. Check “Do not show this message again” and click “Ok”. This is just letting you know that the “RIGHT CTRL KEY” on your keyboard is the “control” key for this virtual machine.

25. “Welcome to the First Run Wizard”, click “Next”

26. “Select Installation Media”, under “Media Source” is a pull down menu. To the immediate right of that pull down menu is an icon with a folder. Click that folder icon.

27. Locate “current.iso” or “dsl-4.4.10.iso” (or the similar file name) that you downloaded. When located, click “Open”. It is likely in the “Downloads” directory of your home folder.

28. Click “Next”

29. Click “Finish”

Now the virtual machine will start to boot up. Simply wait… (This may take up to 5 minutes.)

30. One or more new dialogs may come up saying “VirtualBox Information”, just click “Do not show this message again” and click “Ok”

After a few minutes, the booting will finish and you will be looking at the desktop for your firewall virtual machine. To the right of the window you will see some stats that look something like this:

Up: 0 k/s – Down: 0 k/s

Processes: 19

CPU Usage: 10%

RAM Usage: 16.2MB/28.8MB

etc.

Congratulations! You now have a firewall running. Now we will set up this firewall to protect you so that you can safely use TOR from your main virtual machine.

=== 10. Firewall Configuration ===

At this stage you should be looking at the desktop for “DSL” (Damn Small Linux).

I need to talk about the mouse first. This particular virtual machine, as well as your main operating system (windows) both wants control of your mouse. Both cannot have control of your mouse at the same time however. Therefore, you have to choose whether the mouse will be used by your virtual machine, or by Windows. When you click into your virtual machine, it has the effect of passing control of the mouse to the virtual machine. That means you cannot move your mouse cursor past the boundaries of that virtual machine. In order to give mouse control back to windows, enabling you to move your mouse cursor anywhere, simply press the right ctrl key on your keyboard. That is to say, you have two ctrl keys. One on the left of your keyboard and one on the right. Press the ctrl key that is on the right of your keyboard. This will give mouse control back to windows.

Practice this a bit. Practice clicking into the window, moving the mouse cursor around, pressing right ctrl, and moving the windows mouse cursor around. Get the feel of it.

You should see a window that looks something like a web browser, with some text in it including words such as “Getting Started with DSL”. First, close that window.

(If your mouse is not working, read this mini-section.)

(First, click inside the window that your virtual machine is running in). Now try moving your mouse cursor. If you do not see the mouse cursor moving around, then press (RIGHT CTRL + I). Now move your mouse cursor again. If you notice that you are moving your “main” mouse cursor over the window, but you do not see the “DSL” black mouse cursor moving, then click again into that window. If you do this a few times, you should notice that the mouse begins to work. You may have to press RIGHT CTRL+I a couple of times to get the mouse to work.

1. Once the mouse is working inside of your virtual machine, go ahead and close the window entitled “Getting Started with DSL”

> (If you cannot see the full virtual machine window, for example because your screen resolution is set so that some of the window goes too low, read this mini-section).
>
> (First, press RIGHT CTRL+I until you have your main windows white mouse cursor back). Now, click on “Machine” in the menu at the top of the window.

(Select “Switch to Scale Mode”)

(Click “Switch”)

(Now you will have converted your firewall window to a smaller size, and you will be able to resize it. You may need to press “right ctrl” to get a windows mouse cursor (which you will need in order to resize this window). Now simply resize it to the size that works for you, and then click into the window to be able to use the black mouse cursor inside the virtual machine. I recommend you maximize this window to make sure you can read everything clearly.

2. Right click anywhere on the desktop, go to System (a red folder), go to Daemons, ssh, and start.

3. Right click again anywhere on the desktop, go to XShells -> Root Access -> Transparent

4. Now you have a window that you can type in. Type exactly as shown below into this window and hit enter:

passwd

Once you type this and hit enter, it will ask you for a password. This is a password for full access to the firewall. Make it at least 8 characters in size.

*** IMPORTANT: Do not forget your firewall password. You will need it later in the guide. ***

When you have successfully changed your password, it will say “Password changed.”

5. Now type exactly as shown below, into the same window:

ifconfig eth1 10.0.3.1

6. It will not say anything after you hit enter; it will just return you back to the prompt.

Now our firewall server is ready. We want to save this state so that we can get back to it easy in the future.

Press RIGHT CTRL+S

7. Now you will be looking at a window that says “Take Snapshot of Virtual Machine”. Just click “Ok”

8. Now, let’s test this out to confirm it works as we expect. Go ahead and close the virtual machine by clicking the “X” in the top right corner. A menu will come up. Select ”Power off the machine” and click ok. Do NOT check the box called “Restore current snapshot”.

And now you should be once again at the VirtualBox manager. You will see “Firewall (Shapshot 1), Powered Off”

9. Make sure that “Firewall (Snapshot 1), Powered Off” is selected. At the top right of your VirtualBox Manager is a button that says: “Snapshots (1)”. Click it.

10. Click on “Snapshot 1″, the top-most selection. This will highlight it.

11. Now right click it, and click on “Restore Snapshot”

12. A dialog box will come up asking if you are sure, click “Restore”

13. Now click the “Start” button at the top with the large green arrow.

14. Any dialog boxes that come up with a check box saying “Do not show this information again”, simply check the check-box, and click ok. Do not worry about any of those.

Remember, if you do not have immediate control of the mouse inside the virtual machine, simply press RCTRL+I (press right ctrl and “I” at the same time) and click into it until you have mouse control.

Now your firewall is good to go. Any time you need it, just go to the VirtualBox Manager and follow steps 9 through 14 above. You do not have to go through the whole setup process again at any time in the future. Your firewall is ready.

=== 11. Installing Ubuntu ===

Now we are going to set up the main machine that you will be using TOR with.

1. First, go to this URL: http://www.ubuntu.com

2. Click on the link “Download Ubuntu”

3. Click “Start Download” (This download should take 10-15 minutes)

4. The filename is going to be similar to: ubuntu-10.10-desktop-i386.iso

Now we wait…

While you are waiting for the file to download, go ahead and make sure that your “hidden volume” is mounted in TrueCrypt to a particular drive letter. For example, O: You will need that for the next step.

5. Return to your “VirtualBox Manager”. It doesn’t matter if the firewall is running or not.

6. Click “New” (the blue round star-icon in the top left) again.

7. “Welcome to the New VirtualMachine Wizard”, click “Next”

8. “VM Name and OS Type”, under “Name”, type “Primary”

9. Next to “Operating System”, select “Linux”

10. Next to “Version”, select “Ubuntu” and Click “Next”

11. “Memory”, by default it selects 512 MB. This is fine. 256 MB is the MINIMUM. The more memory you allocate, the better the virtual machine will function. Click “Next”

12. “Virtual Hard Disk”, Make sure “Boot Hard Disk” is checked. Make sure “Create new hard disk” is selected. Click “Next”

13. “Welcome to the Create New Virtual Disk Wizard”, click “Next”

14. “Hard Disk Storage Type”, select “Fixed-size storage” and click “Next”

15. “Virtual Disk Location and Size”, to the right of the text box containing “Primary” is a folder icon. Click the folder icon.

16. Now we have to select a file for the new hard disk image file. On the bottom of this dialog it says “Browse Folders”, click on that.

17. Now click on “Computer” in the menu to the left.

18. Scroll to where you see the drive letter you mounted, and double click on it. Ex: Local Disk (O:)

19. Now click “Save”

20. By default 8.00 GB are selected. That is fine. If you have enough space on your hidden volume, increase this to 10 GB. Otherwise, 8 is fine.

21. Under “Location”, it should say O:Primary.vdi where O: is replaced by whatever drive letter you mounted your TrueCrypt hidden volume to.

22. Click “Next”, then click “Finish”

Now we wait for VirtualBox to create the hard drive we asked for. This may take a few minutes.

Keep in mind this entire virtual machine as well as any of its contents is going to reside within the hidden TrueCrypt container. This ensures extra security.

23. When this is done, you will see a “Summary” window. Click “Finish”.

24. Now, right click on “Primary, Powered Off” in your “VirtualBox Manager”, and click “Start”

25. Again we are at the “First Run Wizard”, click “Next”

26. “Select Installation Media”, under “Media Source” is a pull down menu. Click the “folder icon” to the immediate right of that pull down menu.

27. Locate “ubuntu-10.10-desktop-i386″ (or the similarly named file) from your Downloads directory, or wherever you saved it. Click on it, and click “Open”

28. Click “Next”

29. Click “Finish”

Now simply wait. Your Ubuntu virtual machine will be loading up. This may take a few minutes. Don't worry if you see all kinds of strange messages/text. It is normal.

After a few minutes, you should start to see the Ubuntu desktop load. Unlike your firewall, you will notice that you do not have to click the mouse inside the window. It automatically happens. This is going to be much easier than the "Firewall" step.

Once everything has loaded, you will be looking at a window that says "Install" with a button that says "Install Ubuntu". If you cannot see everything press RCTRL+F (to go full screen). You can return to windowed mode by RCTRL+F again. Any dialogs can be closed, and you can check the box that says "Do not show me this again."

30. Click "Install Ubuntu"

31. Check "Download updates while installing"

32. Check "Install this third-party software". Click "Forward"

33. Ensure "Erase and use entire disk" is selected, and click "Forward". Remember, this is NOT talking about your hard disk. It is talking about the 8-10 gigabyte virtual disk.

34. Click "Install Now"

35. Now you will be guided through a series of installation related screens. The first screen asks you to select your time zone/time. Select your choice and click "Forward"

36. Now keyboard layout, again select your choice and click Forward. If you are unsure, leave it as is or click "Figure out keyboard layout"

37. "Who are you?" For "Your name" type in: mainuser

38. When you type in "mainuser" the other boxes will fill in automatically. Now click in the text box next to "Choose a password".

39. Do NOT use the same password as the firewall. Come up with a different password.

40. Ensure that "Require my password to log in" as well as "Encrypt my home folder" are selected and checked and proceed.

Now simply wait until the installation is finished. The installation may take a while, and it may appear to stall at some points. As long as the ubuntu mouse cursor shows an animation that is turning around in circles, the installation *is* working. Simply wait until it is done. If after an hour or two the progress bar hasn't moved at all, then go ahead

and re-start the installation starting from step 24 (after closing the window and powering down the virtual machine).

Depending on your computer, it could take 2-4 hours. Most likely, it will take about an hour. Once finished, you will see a dialog that says “Installation Complete” with a button that says “Reboot Now”. Do NOT press the “Reboot Now” button. Close the ‘X’ on this window, and Power Down.

41. Now, right click “Primary” and go to “Settings”.

42. Click on “Storage” in the left menu. Then click on the “ubuntu-10.10… .iso” under where it says “IDE Controller”

43. To the right it says “Attributes” under that it says “CD/DVD Drive : …” to the immediate right of that is a cd icon. Click it.

44. Select “Remove disk from virtual drive.”

45. Click “Ok”

46. Now, making sure that “Primary” is highlighted, click the “Start” button at the top with the large green arrow.

Now we wait for your newly installed Ubuntu machine to boot up.

47. After a few minutes, you will see a dialog appear that says “mainuser-VirtualBox”. Go ahead and click on “mainuser” which has the “person icon” to the left of it.

48. Now it will prompt you for your password. Enter the password you used in the installation process.

49. After a minute or so, you should hear a nice login sound, and you should be fully logged into your virtualmachine.

50. Keep waiting, and a dialog will appear that says “Information avialable” and “Record your encryption passphrase” Click on: “Run this action now”

51. Type in the same password you used to log in. After that window closes, click “Close” in the dialog box.

Congratulations! You have now set up a virtual machine as well as a firewall to protect it. Now we need to finish configuring the primary virtual machine.

=== 12. Ubuntu Initial Setup ===

Ok, now that we have installed Ubuntu, we need to set it up so that we can use it fully. This also means making sure we can see flash on websites such as youtube.

1. First, we have to install any updates that are pending. At the bottom of your screen, you should notice where it says “Update Manager”. Click on that.

2. Now, click on “Install Updates”. If you did not see “Update Manager”, then skip these two steps.

3. Any time an administrative task is required, you will need to type in your password. This is the same password you used to log in.

Now we wait, this is going to download any necessary security updates to make certain we are using the most current/secure setup possible. This may require downloading hundreds of megabytes. Just go ahead and let it do that, and when everything is downloaded and updated, proceed to the next step. While you wait, Ubuntu may go into screensaver mode. If so, just move the mouse and it will ask you for your password. That will leave screensaver mode.

If the updates are more than a hundred megabytes, it will take quite a while. It may take up to 2-3 hours depending on your computer and internet connection. Nonetheless, this step is critical. Do not skip the updates. Besides ensuring that your setup will be secure, the updates also ensure that all of the applications are up to date and thus most likely to function correctly. Just go ahead and watch a movie for a couple hours, and then return and check on it.

After all of the updates have been downloaded and installed, the “Update Manager” window will now say “Your system is up-to-date” at the top. Further, it will say: “The computer needs to restart to finish installing updates.”. Go ahead and press the ‘X’ in the top right corner of the window, and choose ‘Send the shutdown signal”. If prompted, click “Shut Down”. Once it has fully shut down, the window will disappear and you will be back at the VirtualBox manager. Go ahead and right click on “Primary” and click “Start”. This will restart the virtual machine.

If a virtual machine fails to shutdown after 10 minutes or so, then go ahead and close the window again by pressing the ‘X’ but this time choose “Power down”. If it still will not shut down, then VirtualBox may have crashed. If so, just follow these instructions:

(Follow the steps in this mini-section if a virtual machine fails to shutdown, or you need to completely close/restart VirtualBox).

(First, press “Ctrl+Alt+Delete”, and then click “Task Manager”). Next, locate the process that is running that starts with “VirtualBox”. Right click that process, and click “End Process Tree”

(This should force the window to close).

(Now, restart VirtualBox by going to your start menu, All Programs, Oracle VM VirtualBox VirtualBOx).

Now you will have the VirtualBox manager up again. To restart the Ubuntu machine, simply right click on “Primary” and click “Start”.

Once your Primary vm has rebooted, you will be again at the login screen. Here as before, click on “mainuser” and then enter in your password. Now your primary machine is fully up to date. Remember, be patient. It may take a few minutes before your virtual machine has fully booted. First you will see the background image and a mouse cursor that can move around, next you should hear the login sound play, and finally you will see the menu at the top and bottom of your virtual machine window. Depending on the speed of your computer, this may take 10 minutes or more. Just be patient. Don’t worry if your virtual machine appears to be running too slow, we will speed it up.

Now your Virtual Machine is set up and ready for use.

=== 13. Installing Guest Additions ===

In order to ensure that the Virtual Machine runs smoothly as possible, we are going to install some additional software to the virtual machine.

1. Go to the “Devices” menu at the top of your virtual machine main window (Machine, Devices, Help), and go to “Install Guest Additions”

2. Go to the “Places” menu at the top of your virtual machine (Applications, Places, System), and click on “VBOXADDITIONS_4.0.4_70112″ (the number may be different).

3. At the top this new window will be the text “The media has been determined as “UNIX software”. Click on “Open Autorun Prompt”

4. A new dialog may appear saying “This medium contains software intended to be automatically started. Would you like to run it?” Click “Run”

5. Enter your administrative password (the one you use to log into Ubuntu) and click “Ok”

6. Now the VirtualBox Guest Additions installer will begin. This may take some time, so just relax and wait. Depending on your computer, this may take 30 minutes or more.

7. When this is finished, you will see the text “Press Return to close this window.” Go ahead and do so.

8. Once that window has closed, go ahead and press the ‘X’ to close the entire virtual machine window. Select “Send the shutdown signal” and click “Ok”.

9. A dialog box will appear. Click on “Shut Down”, the top most option.

At this stage it is a good idea to further optimise our virtual machine. When you initially installed it, you most likely selected either 256 MB or 512 MB of RAM. If you have enough RAM to spare, then I highly recommend you increase that to at least 1 GB. Here is how to do so:

1. First, right click on “Primary, Powered off” and go to Settings.

2. Select “System” from the menu on the left.

3. Increase the “Base Memory” to either 1024 MB (1 GB), or some higher value you are comfortable with.

It is also a good idea to increase the video memory available to the virtual machine.

4. Select “Display” from the menu on the left, still inside of “Settings”

5. Increase the “Video Memory” slider to the right as far as you are comfortable with. For example, 128 MB.

6. Check the box “Enable 3D Acceleration”.

7. Now click “Ok” at the bottom.

Go ahead and start up Ubuntu again by right clicking “Primary, Powered off” and clicking “Start”

When Ubuntu loads up, go ahead and log in as before using your password. Now wait until Ubuntu is fully booted and the “Applications Places System” menu is visible.

You will probably notice that your virtual machine loads up and runs faster than before.

How well your virtual machine runs depends on how good your computer is. Primarily, RAM and processor speed are the most significant factors. If your computer is modern enough, you should be able to use websites with flash and even watch videos, such as on YouTube, with no problem. If your computer is not as modern, you will still be able to browse websites but may not be able to watch videos. You should still be able to use most flash based websites however.

*** IMPORTANT: Do NOT browse sensitive content YET. At this stage, your virtual machine is not yet configured to use TOR. ***

=== 14. Installing IRC (Optional) ===

*** This section is entirely optional. If you are not interested in installing IRC, skip this section. ***

To install IRC on your new virtual machine, follow these steps:

1. Go to the “Applications” menu, and go to “Ubuntu Software Center”

2. Type “kvirc” in the search box field in the top right.

3. When the results return, select the one called: “KDE-based next generation IRC client” or “KV Irc”.

4. Click “Install”

5. Enter your password when prompted.

6. While it installs, you will notice a progress bar. This may take a few minutes depending on the speed of your internet connection.

7. Once it is finished installing, the progress bar will go away. Go ahead and close the “Ubuntu Software Center”.

You are probably used to the close/ min/ max buttons being on the top right, as is the case in Windows. You will find them in the top left instead. If you don’t like this, don’t worry. You can change it later.

Now, let’s go ahead and set up KVIrc.

Remember, you are NOT truly anonymous yet.

8. Click on “Applications” in the top menu.

9. Go to “Internet”

10. Click on “KVIrc”

11. “KVIrc Setup” will appear. Go ahead and click “Next” to begin.

12. “Store Configuration in Folder”, click “Next”

13. “Please choose a Nickname”. You can leave this exactly as is, or you can choose a Nick name then click “Next”.

*** IMPORTANT READ THIS ***

Do NOT pick a nick name you have ever used before, or a nick name that can help someone determine who you are. Also, do NOT fill in any other details such as location, age, real name, etc. Leave everything else as is.

You are NOT Anonymous yet.

14. Now you are asked to pick a theme, select “No theme” then click “Next”

15. Now click “Finish” to leave the KVIrc Setup

16. A new window will appear having a list of servers, click “Close”

Now let’s connect to the “Freenode” IRC network. By now, you may have many questions about how to use Ubuntu. The #Ubuntu chatroom on Freenode is a great place to start, and where you can ask questions related to how to use Ubuntu and VirtualBox. Please remember, you are NOT anonymous yet and anything you say can be matched to your IP address. Keep the conversation related to technical help, or just learning Ubuntu.

Do NOT discuss TOR.

Do NOT discuss ANY sensitive material.

Remember, this chartroom consists mostly of people who have set up Ubuntu for other reasons. Therefore, they will be able to help you configure it, and answer many questions about how Ubuntu works.

17. At the bottom right of KVIrc is a long text input box. Click inside that box.

18. Type, exactly as shown below, including the “/” character:

/server irc.freenode.net 6667

19. This will connect you to the Freenode IRC network. After a few minutes, you will be connected and a dialog box will appear.

20. Uncheck the box that says “Show this window after connecting”, and then click “Close”

21. Now, in the same text box as you typed the /server command, type the following exactly as shown below, including the “/” and “#” characters:

/join #Ubuntu

22. Now you are in the #Ubuntu chatroom. Feel free to discuss the Ubuntu operating system and ask questions related to how to use Ubuntu. Remember:

*** Do NOT discuss TOR or sensitive material. You are NOT anonymous. ***

This is a good opportunity for you to learn how to set up Ubuntu to be the way you want as far as colors, layout, theme and so forth. When you have finished, simply close the “KVIrc” window.

=== 15. Installing Torchat (optional) ===

*** This section is entirely optional. If you are not interested in installing Torchat, skip this section. ***

Torchat is a program you can use to communicate securely and anonymously with other Torchat users. It is only useful if you already know someone who is using it. If you do not know someone using Torchat, then it is best to skip this section and come back to it in the future when you want to install Torchat.

These instructions work for Ubuntu 10.10.

First, installing Torchat is a bit tricky because Ubuntu does not include Tor by default in its repositories. Tor is a requirement for torchat, and therefore we have to first install Tor on Ubuntu. Doing so is not too difficult.

1. First, go to “Applications” -> “Accessories” -> “Terminal”. You will see a new window appear with a prompt that looks like this:

mainuser@mainuser-VirtualBox:~$

2. Now, type exactly as shown below, and hit enter:

sudo bash

3. After entering your password, you will be at a new prompt which looks like this:

root@mainuser-VirtualBox:~#

4. Now, either type or copy-paste the below text into this window and then hit enter:

echo “deb http://deb.torproject.org/torproject.org experimental-lucid main” | sudo tee -a /etc/apt/sources.list

sudo apt-key adv –keyserver keyserver.ubuntu.com –recv-keys 886DDD89

5. After you do this, you should see the following at the bottom of your window:

gpg: Total number processed: 1

gpg: imported: 1 (RSA: 1)

6. Now, we should be able to install tor. In this same window, type the following commands, one at a time:

apt-get update

apt-get install vidalia privoxy tor

7. (press Y and enter when prompted)

Now we need to obtain the Torchat installation file, follow these steps:

8. In firefox on Ubuntu, go to the following URL: http://code.google.com/p/torchat

9. On the left under where it says “Downloads”

10. One of the files listed will end in .deb, for example torchat-0.9.9.deb. Click on that file name.

11. On the next page, again click on the file name. This should begin the file download.

12. By default, Ubuntu wants to open this file using the “Ubuntu Software Center”. This is correct.

Now wait until the file finishes downloading, and then the “Ubuntu Software Center” will appear. Follow these steps:

1. Press “Install”

2. Type in your password when prompted.

After a short wait, Torchat will be installed.

To start Torchat, go to “Applications” -> “Internet” -> “Torchat Instant Messenger”

=== 16. Creating TOR-Only Internet Environment ===

Up until now, we have been using our Virtual Machine to access the internet directly. This was necessary so that we could install updates, software, and get a feel for how to use Ubuntu.

Now it is time to force Ubuntu to connect to the internet using TOR Only. At the end of this phase, your Ubuntu virtual machine will be usable as a secure and anonymous TOR based browsing environment. It will be *impossible* for you to access the internet except through TOR, and therefore you can rest assured that anything at all you do online through the Ubuntu virtual machine will be through TOR.

First, we need to shut down any running virtual machines. If “Primary” is running, click the ‘X’ in the top right to close it. Select “Send shutdown signal” and then select “Shut Down” when prompted. If “Firewall” is running, go ahead and close it in the same way, but choose “Power off”.

After a minute or so, you should be back to your VirtualBox Manager, with neither virtual machine running.

1. Right click on “Primary, Powered Off” and go to “Settings”

2. Select “Network” from the menu on the left.

3. Next to “Attached to” is a pull down menu. Right now it is set to “NAT”. Choose “Internal Network” and click “Ok”

4. Click “Firewall” to highlight it, and then click on “Snapshots (1)” in the top right.

5. Right click on “Snapshot 1″ and then select “Restore Snapshot”. Select “Restore” if prompted.

6. Right click “Firewall” and click “Start”

Now your Firewall will be resumed exactly where it had been previously set up. The last command entered should still be visible.

Before you proceed, make sure that TOR is running on your main Windows computer. If it is, you will see an “Onion” icon visible in your task bar. Click on that icon and you should see the “Vidalia Control Panel”. Make sure that it says “Connected to the TOR

Network". If so, you are ready to proceed. If not then please see section 2 : "Using and Testing Tor Browser for the first time" to re-start TOR. Once TOR is running, proceed.

Let's restart Ubuntu:

7. Right click "Primary" and click Start. Log in as normal.

8. After fully logged in, open "Firefox" by clicking the orange "Firefox" logo at the top, next to "System".

9. Try to go to any website, such as http://www.google.com. Try at least 3-5 different websites. You should not be able to connect to any of them.

Note: If you attempt to go to websites you have already been to using Ubuntu, they may appear to load because they are cached.

10. In Firefox on Ubuntu, go to "Edit" and "Preferences"

11. Click on the "Advanced" icon

12. Click on the "Network" tab

13. Under "Connection" it says "Configure how Firefox connects to the internet". To the right of that is a "Settings" button. Click that button.

14. Select "Manual proxy configuration"

15. Next to both "HTTP Proxy" and "SSL Proxy" type in: 127.0.0.1

16. Set the port to 8118 for both "HTTP Proxy" and "SSL Proxy"

17. Next to "SOCKS Host" type: 127.0.0.1

18. Set the port for "SOCKS Host" to 9050

19. Make sure that "SOCKS v5″ is selected at the bottom.

20. Click "Ok" and then "Close"

Now we have instructed Firefox to use TOR. However, Firefox cannot use TOR yet. Right now, Ubuntu is completely unable to connect to the Internet. We are going to change that.

21. Go to “Applications” -> “Accessories” -> “Terminal”

22. Type in: sudo bash (and hit enter)

23. Type in your password if prompted.

24. Type in the following commands exactly as shown below (or copy paste them):

ifconfig eth0 10.0.3.2

/etc/init.d/polipo stop

/etc/init.d/tor stop

/etc/init.d/privoxy stop

(Note: the last three commands, those beginning with /etc/ are only necessary if you installed Torchat)

Now you have told your Ubuntu machine to join the same network that your Firewall is on. Now we can establish a tunnel for TOR data to flow from our Ubuntu machine, through the Firewall, into your Windows guest machine. We need to establish two such tunnels.

The first tunnel for port 9050 data, and the second tunnel for port 8118 data. When these two tunnels are set up, it will be possible for you to use your Ubuntu machine to access any website using TOR. Further, it is still completely impossible for your Ubuntu machine to access the Internet in any other way.

25. Your terminal window should still be open. Type in the following command exactly as shown (or copy paste it):

ssh -N -L 9050:10.0.2.2:9050 root@10.0.3.1

26. Type “yes” if prompted. When prompted for the password, give your Firewall password. Not your Ubuntu password.

After you hit enter, you will see the cursor go to a blank line and nothing else happens. This simply means the connection you requested is active. If the connection were to stop for any reason, you would return to a command prompt. If you want to terminate the connection yourself, simply hit CTRL+C. You can type in the same ssh command again if you need to re-open the tunnel.

27. Now we are going to open the second tunnel. In your terminal window, go to “File” and “Open Tab”. This will open up a tab for a second terminal without affecting the first.

28. Now, type exactly as shown below to open the second tunnel:

ssh -N -L 8118:10.0.2.2:8118 root@10.0.3.1

29. Return to Firefox. Go to the “File” menu and uncheck “Work Offline” if it is checked.

30. Go to the URL: http://check.torproject.org

If you see the text: “Congratulations. Your browser is configured to use Tor” then you are all set! Your Ubuntu virtual machine is now NOT connected to the internet in any way. However, you can browse any website using TOR, even Youtube. You do not have to be afraid of javascript or Flash. Any files you save onto your virtual machine will automatically be saved in the encrypted truecrypt volume you set up earlier. In fact, everything the virtual machine does will be contained within that truecrypt volume.

Further, even if someone somehow managed to remotely gain full root access to your Ubuntu machine (absurdly unlikely to happen), they would still not be able to see *anything* about who you are, or what your real IP address is, or even that you are using a Virtual Machine. To them, it would appear that the Ubuntu machine is your main computer. They would be totally unable to compromise your identity based on this alone.

However, keep the following in mind. If someone were to gain access to your Ubuntu machine, they WOULD be able to see anything you have used it for or any files you have saved. Therefore, I recommend for the sake of absolute security, do not store anything on your Ubuntu virtual machine that identifies you. This is just a precaution. It is virtually impossible that someone would manage to remotely gain access to your Ubuntu machine.

=== 17. General Daily Usage ===

Much of this guide has involved detailed one-time setup processes. From now on, all you have to do when you want to use TOR from your Ubuntu virtual machine is to follow these steps. Every step listed is a step you have already done, so feel free to re-visit earlier sections if you need help.

1. Start TrueCrypt, and mount your hidden volume which contains your virtual machine.

2. Start VirtualBox

3. Start TorBrowser Bundle.

4. Click “Firewall” to highlight it, and then click on “Snapshots (1)” in the top right.

5. Right click on “Snapshot 1″ and then select “Restore Snapshot”. Select “Restore” if prompted.

6. Right click “Firewall” and click “Start”

7. Right click “Primary” and click Start. Log in as normal.

8. Go to “Applications” -> “Accessories” -> “Terminal”

9. Type in: sudo bash (and hit enter)

10. Type in your password if prompted.

11. Type in the following commands exactly as shown below (or copy paste them):

ifconfig eth0 10.0.3.2

/etc/init.d/polipo stop

/etc/init.d/tor stop

/etc/init.d/privoxy stop

(Note: the last three commands, those beginning with /etc/ are only necessary if you installed Torchat)

12. Your terminal window should still be open. Type in the following command exactly as shown (or copy paste it):

ssh -N -L 9050:10.0.2.2:9050 root@10.0.3.1

13. Type “yes” if prompted. When prompted for the password, give your Firewall password. Not your Ubuntu password.

14. In your terminal window, go to “File” and “Open Tab”.

15. Now, type exactly as shown below to open the second tunnel:

ssh -N -L 8118:10.0.2.2:8118 root@10.0.3.1

16. Return to Firefox. Go to the “File” menu and uncheck “Work Offline” if it is checked.

17. Go to the URL: http://check.torproject.org

If you see the text: “Congratulations. Your browser is configured to use Tor” then you are all set!

Enjoy!

Phew, now i have it completed! I admit its quite extensive, not to say enormous, but its the best how-to on anonymity and other safety procedures i have found so far. It secures your sys black-hat style^^ :

http://en.wikipedia.org/wiki/Black_Hat_Briefings (for those of you who don’t know black hat ^^)

You dont have to do all steps at once. You can do a little of it every time you have an hour or two to spare. I think for the whole procedure you will need roughly 8-12 hours. I think its written in a way everybody should be able to follow. If there are still steps unclear just ask, i will see if i can help you. btw this is written for noobs, but the tips here are interesting for almost everybody.

P.S.: Once you have installed TOR you can get access to TOR hidden services and other interesting deep-web pages. If you want some links for your first steps into this hidden part of the internet just ask me. If there are a lot of requests i will write an extra thread with the most important websites in the deep web. One thing before you get started: most deep web pages aren't online 24/7. So if you can't reach a certain website be patient and try again and again till you get access. Another thing: you will find websites that are pretty shocking and disturbing. In 99.5% you will see beforehand what you find on those sites, so if you dont want to see certain things don't click on the links.

Now that you have a really secure system, you should know what to do when the shit hits the fan and you are arrested or your home gets searched. Your system, is secured in a way they cant break, so the only thing that can incriminate you now is your testimony.

These 2 YouTube videos are 2 lectures on behavior towards the police in such situations. Part one is done by a criminal defense attorney, part 2 by a very experienced police officer. They both tell you about the tricks the police uses and how you should react:

https://www.youtube.com/watch?v=6wXkI4t7nuc&feature=player_embedded

https://www.youtube.com/watch?v=08fZQWjDVKE&feature=player_embedded

Always say nothing and ask for a lawyer, ALLWAYS ! You cannot improve your situation with anything you say (this is counterintuitive, but the attorney here has in his whole carrier NEVER heard of single case where a suspect could help his case by talking to the police, but he could name many cases where they made matters way worse) but you can make it a lot worse, so shut the hell up and wait for your lawyer.

Even him being a defense lawyer wouldn't talk to the police under any circumstances. You can tell your story before court AND NEVER, UNDER NO CIRCUMSTANCES, BEFORE THAT ! Even the cop in lecture 2 says NEVER TALK TO THE POLICE!!!!!

=== END ===